IX kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 77)**

z dnia 6 lipca 2022 r.

Pełny zapis przebiegu posiedzenia

Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 77)

6 lipca 2022 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Grzegorza Napieralskiego (KO)**, zastępcy przewodniczącego Komisji, rozpatrzyła:

– informację ministra cyfryzacji na temat realizacji Strategii Cyberbezpieczeństwa na lata 2019–2024.

W posiedzeniu udział wzięli: **Janusz Cieszyński** sekretarz stanu w Kancelarii Prezesa Rady Ministrów, pełnomocnik rządu do spraw cyberbezpieczeństwa, **Jacek Oko** prezes Urzędu Komunikacji Elektronicznej wraz ze współpracownikami, **Jacek Kosiorek** wiceprezes Polskiej Izby Radiodyfuzji Cyfrowej, **Bartosz Sowier** dyrektor Departamentu Analiz i Legislacji Pracodawców Rzeczypospolitej Polskiej wraz ze współpracownikami, **Sylwester Szczepaniak** koordynator do spraw społeczeństwa informacyjnego i smart city Unii Metropolii Polskich, **Joanna Karczewska** członek Stowarzyszenia ISACA Warszawa, **Robert Śmietanka** i **Artur Pająk** eksperci Polskiej Izby Informatyki i Telekomunikacji, **Michał Smagowicz** członek zarządu Thinktank sp. z o.o. oraz **Radosław Nielek** stały doradca Komisji. W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Magdalena Krzymowska** i **Wioletta Więciorkowska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dzień dobry. Witam bardzo serdecznie. Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

Stwierdzam kworum oraz przyjęcie protokołu z poprzedniego posiedzenia Komisji wobec niewniesienia do niego zastrzeżeń.

Witam bardzo serdecznie posłów zgromadzonych na sali oraz gości biorących udział w naszym posiedzeniu. Kancelarię Prezesa Rady Ministrów reprezentuje pan minister Janusz Cieszyński, sekretarz stanu w KPRM, dzień dobry panie ministrze. Witam serdecznie.

Sekretarz stanu w Kancelarii Prezesa Rady Ministrów, pełnomocnik rządu do spraw cyberbezpieczeństwa Janusz Cieszyński:

Dzień dobry.

Przewodniczący poseł Grzegorz Napieralski (KO):

Witam bardzo serdecznie pana prezesa Jacka Oko, prezesa Urzędu Komunikacji Elektronicznej. Dzień dobry panie prezesie, witam bardzo serdecznie. Jest z nami również pan Jan Sołyga, pełniący obowiązki naczelnika w Departamencie Bezpieczeństwa Urzędu Komunikacji Elektronicznej. Dzień dobry, witam pana bardzo serdecznie. Polska Izba Informatyki i Telekomunikacji – pan Robert Śmietanka, ekspert. Dzień dobry, panie Robercie, witam bardzo serdecznie. Polską Izbę Radiodyfuzji Cyfrowej reprezentuje pan Jacek Kosiorek, wiceprezes zarządu. Dzień dobry panie prezesie, witam bardzo serdecznie. Stowarzyszenie ISACA Warszawa – Joanna Karczewska, członek stowarzyszenia. Dzień dobry, pani Joanno, witam bardzo serdecznie. Ośrodek Thinktank – Michał Smagowicz, członek zarządu. Dzień dobry, panie Michale, witam bardzo serdecznie. Pracodawców Rzeczypospolitej Polskiej reprezentuje pan Bartosz Sowier, dyrektor Departamentu Analiz i Legislacji – witam bardzo serdecznie – oraz Tomasz Sojka, ekspert. Dzień dobry, witam bardzo serdecznie. Unia Metropolii Polskich – Sylwester Szczepaniak,

koordynator do spraw społeczeństwa informacyjnego i smart city. Dzień dobry. Witam bardzo serdecznie. Witam również stałego doradcę Komisji, pana Radosława Nielka.

Porządek dzisiejszego posiedzenia przewiduje rozpatrzenie informacji ministra cyfryzacji na temat realizacji Strategii Cyberbezpieczeństwa na lata 2019–2024. Czy zgłaszają państwo wniosek do porządku dziennego? Wobec niezgłoszenia wniosku do porządku dziennego stwierdzam jego przyjęcie. Bardzo proszę pana ministra Janusza Cieszyńskiego o przedstawienie informacji. Bardzo proszę.

Sekretarz stanu w KPRM Janusz Cieszyński:

Szanowny panie przewodniczący, szanowni państwo, przekazaliśmy w formie pisemnej informację, ona jest się obszerna, więc postaram się przejść przez najważniejsze elementy, które, myślę, będą takim dobrym otwarciem dyskusji, a później z przyjemnością odpowiem na wszystkie pytania.

Oprócz oczywiście takich działań, które wynikają z *business as usual* w zakresie działalności podmiotów krajowego systemu cyberbezpieczeństwa udało się osiągnąć parę takich celów, które do tej pory nie były zakładane. Jednym z nich było uchwalenie w ubiegłym roku i wdrożenie ustawy o szczególnych warunkach wynagradzania ekspertów z obszaru cyberbezpieczeństwa. To jest ustawa, dzięki której 2 tys. osób już dzisiaj, które spełniają formalne warunki określone w rozporządzeniu, wydanym na podstawie tej ustawy, może liczyć na dodatkowe wynagrodzenie. I to jest, szanowni państwo, nasza odpowiedź na to, jak wygląda aktualnie sytuacja na rynku, jeżeli chodzi o ekspertów w dziedzinie cyberbezpieczeństwa. W ubiegłym tygodniu ukazał się raport, z którego wynika, że w ciągu ostatnich 9 lat na świecie przybyło około 2,5 miliona etatów osób zatrudnionych w dziedzinie cyberbezpieczeństwa, z czego milion jest nieobsadzony. Było około miliona, teraz jest 3,5 miliona osób na całym świecie, które by chciano zatrudnić na tych etatach. Widzimy, że w tym coraz trudniejszym środowisku, coraz trudniejszym otoczeniu państwo polskie zyskało instrument do tego, aby aktywnie prowadzić politykę kadrową i być w stanie nie tylko pozyskać nowych ekspertów, ale też utrzymać tych, którzy już dla Polski pracowali i zaoferować im atrakcyjne, zbliżone bardziej do rynkowych wynagrodzenia.

Oprócz tego myślę, że niezwykle istotnym elementem realizacji strategii w tym obszarze ministra obrony narodowej było powołanie dowództwa komponentu Wojsk Obrony Cyberprzestrzeni w oparciu o Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni. Ale trzeba powiedzieć bardzo jasno, że jeżeli chodzi o ten obszar sił zbrojnych, w cyberbezpieczeństwie są bardzo duże postępy w ostatnich latach i aż przyjemnie patrzeć, jak ten element się rozwija. Także tutaj wielkie gratulacje dla Ministerstwa Obrony Narodowej i wszystkich, którzy za to odpowiadają, z samym generałem Karolem Molendą na czele. Oprócz tego cały czas trwają prace legislacyjne nad innymi istotnymi aktami prawnymi. Niedawno skierowaliśmy do rozpatrzenia kolejne projekty, między innymi projekt, który ma na celu przeciwdziałanie nadużyciom w komunikacji elektronicznej. To jest odpowiedź na sytuację, z którą mieliśmy do czynienia w ostatnich miesiącach w coraz większym stopniu, czyli zagrożenia spoofingiem, phishingiem, smishingiem – takimi nadużyciami w komunikacji elektronicznej, które wprost uderzają w obywateli. Do tej pory było tak, że dla wielu cyberbezpieczeństwo było domeną wyłącznie ekspertów, jakichś bardzo skomplikowanych systemów. Dzisiaj widzimy, że to jest coraz większy problem dla zwykłych obywateli. Stąd też decyzja o powołaniu Centralnego Biura Zwalczania Cyberprzestępczości. Ta formacja funkcjonuje już od początku tego roku.

Trwają prace nad ustawą o krajowym systemie cyberbezpieczeństwa. To jest kompleksowa regulacja, która oprócz kwestii związanych z nowelizacją tych przepisów, które do tej pory były w zakresie ustawy o krajowym systemie cyberbezpieczeństwa, dodaje też bardzo ważny rozdział dotyczący bezpiecznej sieci łączności rządowych, sieci, która byłaby oparta o pasmo 700 MHz. Cały czas trwają też prace, które mają na celu skonsolidowanie tego sektora cyberbezpieczeństwa. Czyli tutaj rozbudowujemy z jednej strony współpracę w ramach struktur państwowych, a z drugiej w ramach programu PWCyber otwieramy się coraz bardziej na świat zewnętrzny. Coraz więcej partnerów firm krajowych, ale też międzynarodowych do tego programu dołącza. Rozbudowujemy zespoły

reagowania na incydenty bezpieczeństwa komputerowego. Powstają też kolejne ISAC-i. Tutaj też jest z nami pan prezes Jacek Oko z Urzędu Komunikacji Elektronicznej. Taki ISAC dla sektora telekomunikacyjnego w UKE funkcjonuje. Myślę, że to też dobrze pokazuje, że w tym obszarze najważniejsze jest nie tylko to, żeby były jakieś przepisy, ale też to, żeby po prostu była chęć. Tu chciałem bardzo serdecznie podziękować panu prezesowi za tę inicjatywę, bo między innymi w ramach tej inicjatywy powstały szczegółowe założenia tej ustawy, o której przed chwilą mówiłem. Myślę, że też warto powiedzieć o tym, że na cyberbezpieczeństwo – teraz pracujemy nad przeglądem tej strategii i to będzie jeden z jej elementów – w końcu łożymy znacznie więcej środków niż do tej pory. Kilka tylko elementów w ramach programu Cyfrowa Gmina… Około 100 mln zł w tym roku trafiło do samorządów właśnie na cele związane z cyberbezpieczeństwem. W ramach wspólnie realizowanego z Narodowym Funduszem Zdrowia i Ministerstwem Zdrowia programu rozbudowy zdolności w zakresie cyberbezpieczeństwa w szpitalach – 0,5 mld zł na zabezpieczenie systemu ochrony zdrowia. Oprócz tego dodatkowe środki na wynagrodzenia, o których mówiłem, to jest około 170 mln zł w tym roku. Zwiększenie o 100% dotacji podmiotowej dla CSIRT NASK, rozbudowa też innych systemów właśnie z obszaru cyberbezpieczeństwa, między innymi systemu komunikacji niejawnej. Jak nie uda się zbudować tego operatora sieci bezpieczeństwa, to rozbudowa tych rozwiązań, które już wcześniej powstały w Agencji Bezpieczeństwa Wewnętrznego na kolejne instytucje.

Tak naprawdę można powiedzieć, że jeżeli chodzi o ten wymiar finansowy, w tym roku myślę, że około 800 mln zł więcej niż w roku ubiegłym w sektorze cywilnym – mówię tutaj o ABW, o służbach i o NASK – na te cele wydamy. Myślę, że to jest duża zmiana. W ramach Ministerstwa Obrony Narodowej te wydatki też stale rosną. Bardzo ambitna druga edycja programu CYBER.MIL – też ma w sobie duży komponent inwestycyjny.

Jesteśmy też aktywni na arenie międzynarodowej. Jesteśmy jednym z liderów programu budowy ambasad danych na terenie całej Europy. Jak pewnie część z państwa wie, taką ambasadę danych dziś posiada w Luksemburgu Estonia, natomiast Polska chciałaby – i o to zabiega na poziomie unijnym i tutaj mamy sojuszników – żeby te sprawy uregulować na poziomie całej Unii Europejskiej. Dzięki naszej aktywności udało się też w motywach do NIS2 zawrzeć kwestię nawiązujące do naszego rozwiązania w zakresie funduszu cyberbezpieczeństwa. Czyli tak naprawdę NIS2 będzie mówił o tym, że należy zapewnić finansowanie dla rozwoju cyberbezpieczeństwa. To jest trochę nawiązanie do tego, co pan minister z Estonii zaproponował w ubiegłym roku w ramach tak zwanej deklaracji z Tallina, gdzie zaproponowano, że na wzór wydatków na obronność w NATO powinien być minimalny poziom wydatków na cyberbezpieczeństwo. To jest w pewnym sensie nawiązanie do tego i już jakieś skonkretyzowanie. Właśnie dzięki zabiegom naszych dyplomatów udało się to wprowadzić do tekstu, mimo że pomysł, można powiedzieć, zrodził się na już dość późnym etapie prac nad NIS2. Ta sytuacja, którą mamy w Ukrainie jeszcze nas tylko utwierdziła w przekonaniu wszystkie państwa członkowskie i z dużym zainteresowaniem spoglądają na to rozwiązanie, które wprowadzamy. Myślę, że wielu miejscach, w wielu punktach jesteśmy liderem także na arenie międzynarodowej.

Tutaj też nie sposób nie powiedzieć o działaniach, które realizujemy w związku z wojną w Ukrainie. Wspólnie z ukraińskim ministerstwem transformacji cyfrowej… Myślę, że suma różnych projektów, które zrealizujemy, przekroczy 100 mln zł w tym roku. To są projekty, które podnoszą bezpieczeństwo Ukrainy, które dają możliwość korzystania z technologii, z infrastruktury właśnie w celu zwiększenia bezpieczeństwa ukraińskich systemów. Myślę, że to też jest dobra współpraca i bardzo pożyteczna. Ona pokazuje, że wtedy, kiedy nasi przyjaciele są w potrzebie, to my jesteśmy w stanie na te potrzeby szybko i sprawnie odpowiadać. To są chyba najważniejsze elementy, o których chciałem dzisiaj powiedzieć. Wiele z nich trochę wykracza poza zakres tej informacji. No ale dlatego też uznałem, że skoro tutaj państwo dysponujecie tym dokumentem, to ewentualnie możecie się z nim zapoznać, a takie rzeczy, które się wydarzyły w międzyczasie, to ja po prostu dopowiedziałem. Bardzo serdecznie dziękuję i zapraszam do zadawania pytań.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, panie ministrze, za pana obecność, za przekazanie nam tych informacji i omówienie dokumentu. Chciałbym złożyć na pana ręce taki żal – jeżeli będzie pan rozmawiał z premierem na jakimś spotkaniu – uważam, że ten dokument czy ta dyskusja jest bardzo ważna i na jednej z pierwszych stron mamy informacje dotyczące polskiego wojska, a nikogo z ministerstwa obrony niestety nie ma.

Sekretarz stanu w KPRM Janusz Cieszyński:

Przepraszam bardzo, ja to muszę wziąć w 100% na siebie. Nawet dzisiaj rozmawiałem z panem ministrem Wiśniewskim. Może zabrakło mi skromności, ale zobowiązałem się do tego, że będę także i pana ministra reprezentował podczas dzisiejszego posiedzenia. Pan minister Wiśniewski bardzo chciał dzisiaj być, a ja go namówiłem, żeby nie… Także bardzo, panie przewodniczący, przepraszam i to jest w 100% moja wina.

Przewodniczący poseł Grzegorz Napieralski (KO):

Ministerstwo Obrony Narodowej ma w panu, panie ministrze, bardzo dobrego adwokata.

Sekretarz stanu w KPRM Janusz Cieszyński:

Mówię, jak jest. Byłoby nieuczciwe, gdybym tutaj o tych ważnych okolicznościach nie wspomniał.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję panie ministrze, za przedstawienie informacji. Otwieram dyskusję. Czy ktoś z panów posłów chce zabrać głos? Bardzo proszę. Panie pośle, oddaję głos.

Poseł Fryderyk Kapinos (PiS):

Panie przewodniczący, panie ministrze, szanowni państwo, ja bardzo chciałem podziękować panu ministrowi Januszowi Cieszyńskiemu, który przyjechał na spotkanie z przedsiębiorcami do Mielca na konferencję cyberbezpieczeństwo dla mikro, małych i średnich przedsiębiorców z ekspertem z NASK, panem Kamilem Kuciem… W konferencji wzięli udział również przedstawiciele Policji, naczelnicy, którzy zajmują się cyberbezpieczeństwem. Bardzo ważne, bardzo udane spotkanie i bardzo potrzebne spotkanie, ponieważ szczególnie ci przedsiębiorcy mikro, mali, średni potrzebują rady i takiego roboczego spotkania. Bardzo dziękuję, panie ministrze.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, panie pośle. Czy ktoś z posłów chciałby jeszcze zabrać głos? Ktoś z zaproszonych gości? Jeżeli pan pozwoli, to może od pani Joanny zaczniemy, ustąpimy kobiecie, tak? Bardzo dziękuję. Proszę bardzo.

Członek Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Dzień dobry, nazywam się Joanna Karczewska. Reprezentuję osoby, które na co dzień zajmują się cyberbezpieczeństwem, bezpieczeństwem informacji i ochroną danych osobowych. Zatem dzisiejszy temat jest nam szczególnie bliski. I chciałam się odnieść do kwestii, które poruszył pan minister oraz do innych kwestii zawartych w celach strategii, a które dzisiaj nie zostały poruszone.

Pierwsza rzecz. Wspomniał pan o funduszu cyberbezpieczeństwa, czy on szczególnych chwil zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Otóż mam sygnały od członków naszego stowarzyszenia pracujących w sektorze publicznym – i mówię tu certyfikowanych audytorach, czyli o osobach z najwyższymi kompetencjami – że kryteria przyznawania dodatków są mocno uznaniowe, absolutnie nie zawsze wiadomo, na jakiej zasadzie dodatki są wyliczane. W pierwszej grupie szczególnie widełki są zbyt duże. Bo tam jest między 2 tys. zł a 30 tys. zł. O dziwo tam są właśnie audyty ulokowane. A brakuje certyfikatu CISA w pierwszej grupie. Chcielibyśmy zaproponować chociażby, żeby w taryfikatorze – jak ja to nazywam – audyty były jako oddzielny podpunkt i oddzielnie wycenione. Bo to wydaje nam się mocno dziwne, że osoba, która ma najwyższe kwalifikacje, czyli międzynarodowy certyfikat, ocenia osoby, które na co dzień zajmuje się cyberbezpieczeństwem, ma 2 razy niższy dodatek niż osoby, które audytuje.

Druga kwestia. Zwalczanie cyberprzestępczości i proponowana ustawa o nadużyciach w komunikacji… Bardzo ciekawe. Czekam na wyniki kontroli NIK o nazwie „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości". To nam da duże wyobrażenie o tym, co jeszcze pozostało do zrobienia. To jest też właśnie w ramach celu pierwszego. Cel drugi to między innymi opublikowanie narodowych standardów cyberbezpieczeństwa, które obowiązują od 1 września 2021 r. Napisałam opinię w czasopiśmie, mam nadzieję, że pan się z nią zapoznał. Ale co jest dla nas bardzo istotne? Oprócz kiepskiej jakości tłumaczeń, to są pytania, które ja zadałam. Bardzo liczymy na odpowiedź. Jak narodowe standardy cyberbezpieczeństwa mają się do rozporządzenia o KRI? Jak mają się do innych metod? Szczególnie tutaj jest narodowy standard – ramy zarządzania ryzykiem. Jak się ten standard ma do innych metodyk zarządzania ryzykiem? Ja je wymieniam w swoim artykule. Oraz jak i kiedy zostaną narodowe standardy cyberbezpieczeństwa uwzględnione w szablonach audytu w zgodności z ustawą o krajowym systemie cyberbezpieczeństwa? Czy w ogóle były uwzględnione w diagnozie cyberbezpieczeństwa – czyli w bardzo cennej inicjatywie, która jest związana z cyberbezpieczeństwem w samorządach? Prowadzone są prace w ramach konkursu Cyfrowa Gmina. Chciałam też zwrócić uwagę, że tam o mało nie doszło do naruszenia praw autorskich własności intelektualnej naszego stowarzyszenia. Naprawdę, brakowało niewiele. A wie pan sam, panie ministrze, jak bardzo Amerykanie – również moje stowarzyszenie międzynarodowe ISACA – są wyczuleni na ochronę praw autorskich i własności intelektualnej. Chciałam tutaj podziękować pani dyrektor Pogorzelskiej z Centrum Projektów Polska Cyfrowa, która zareagowała natychmiast na mój sygnał o możliwości naruszenia praw autorskich. Niestety na NASK nie mogłam liczyć w tej sprawie.

Kolejny punkt też dotyczy właśnie stanu cyberbezpieczeństwa. Nie dalej jak w kwietniu na posiedzeniu Komisji mieliśmy przedstawione wyniki kontroli „Organizacja pracy zdalnej w wybranych podmiotach wykonujących zadania publiczne w związku z ogłoszeniem stanu epidemii". I to był kolejny raport NIK, który wskazywał na poważne braki w cyberbezpieczeństwie. To, co nas najbardziej zmartwiło, to brak audytów. Przeprowadzono w trakcie kontrolę NIK w zaledwie pięciu kontrolowanych podmiotach, co stanowi 13%. Ten audyt nadal jest postrzegany jako coś zbytecznego. No dobra, zrobimy, ale tak już siłą rozpędu albo właśnie jak NIK wejdzie. Powiem też, że ja często przeglądam raporty z kontroli zarządczej. To jest bardzo ciekawa lektura dostępna bez ograniczeń na stronach jednostek. Znalazłam jedno ze sprawozdań z kontroli zarządczej jednego z ministerstw. Okazało się – oni to szczerze przyznali – że przez 5 lat nie przeprowadzili żadnego audytu bezpieczeństwa. Tutaj bardzo bym prosiła, żeby nalegać, wymagać, niemalże zmuszać do tych audytów, pomimo zapisów w odpowiednich przepisach polskiego prawa.

Przy okazji chciałam spytać. W ramach badania ewaluacyjnego bazy wiedzy, cyberbezpieczeństwa oraz narodowych standardów cyberbezpieczeństwa zostało zadane pytanie, następujące. System zarządzania bezpieczeństwem informacji w tej organizacji jest… Jedna z odpowiedzi do wyboru – poddawane cyklicznej ocenie przez akredytowanego audytora. Może to jest to, co myli. Bo ja nie słyszałam o żadnych akredytowanych audytorach. Ja słyszałam – i sama jestem – o certyfikowanych audytorach. Natomiast nie wiem, skąd się pojawiło pojęcie akredytowanego. Być może to wprowadza w błąd i powoduje zamieszanie. Na polskim rynku w ogóle może nie być akredytowanych audytorów.

Kolejna bardzo niepokojąca sprawa to są wyniki badań wykonanych na zlecenie serwisu Chroń PESEL i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych. Nie wiem, czy pan zna wyniki, ale one są porażające i przerażające, bo wychodzi na to, że wiedza na temat bezpieczeństwa danych osobowych w Polsce oraz cyberzagrożeń – czyli czego boją się Polacy – jest nikła. Na dodatek oba badania pokazują, że się niewiele zmienia. Już pomijam, że jak krew w piach poszły starania – albo też brak starań – przez ostatnie 4 lata wprowadzenia odpowiedniej ochrony danych osobowych. RODO obowiązuje już 4 lata plus 2 lata przed. W sumie 6 lat i nie ma wyników. Na dodatek badania Krajowego Rejestru Długów potwierdzają się w badaniu – poziom wiedzy

finansowej Polaków 2022 – przeprowadzonym przez Fundację Warszawski Instytut Bankowości i Fundację Giełdy Papierów Wartościowych. I tam jest stwierdzenie – ponad połowa Polaków odczuwa brak wiedzy w obszarze cyberbezpieczeństwa. Istotnie częściej wskazują go osoby w wieku 25–34 lata. Cyberbezpieczeństwo jest tematem pierwszej potrzeby wymagającym poprawy. Nadal ponad 50% badanych stwierdziło, że nie wie, jak się ochronić. Jest też oczywiście badanie ENISA – Raising Awareness of Cybersecurity. Tam nawet Polska – a konkretnie Departament Cyberbezpieczeństwa Ministerstwo Cyfryzacji wtedy jeszcze – zgłosiła, że z tą świadomością jest kłopot. „*There is a problem in moving from awareness to execution practicality and implementation are always challenges.*" To jest raport z 2021 r., ale badanie było wykonane w 2020. Nadal stoimy w miejscu. Czegoś zdecydowanie brakuje pod tym względem, a jest to cel nr 4 ze strategii.

Jest też bardzo ciekawa kwestia seniorów, której pan nie podniósł. Ostatnio zaczęłam się nią bardzo interesować. Szczególnie po lekturze książki pani profesor Marty Wrońskiej. Okazuje się, że u pani profesor nie ma cyberprzestrzeni, jest tylko przestrzeń medialna. Chociaż jak wynika z bibliografii, dotarła do materiałów NASK i innych rządowych materiałów. A mimo to cały czas posługuje się pojęciem przestrzeni medialnej. Czyli nawet tam jest jak gdyby problem z dotarciem i ujednoliceniem terminologii. A jeżeli nie mamy ujednoliconej terminologii, to reszta też może wprowadzać w błąd. Śledzę obecnie kursy prowadzone w ramach programu wieloletniego na rzecz osób starszych – aktywni plus. I to są zajęcia prowadzone, pilotowane przez Ministerstwo Rodziny i Polityki Społecznej. Mam pytanie, czy w ogóle jest jakieś śledzenie, co jest proponowane seniorom w trakcie kursów? Była przecież inicjatywa Komisji i stanowisko z 7 grudnia ub.r. Zgłosiłam gotowość naszych seniorów, z naszego stowarzyszenia. Byłam także w kontakcie z kolegami z Polskiego Towarzystwa Informatycznego i oni też okazali się być bardzo zainteresowani współpracą w ramach uświadamiania seniorów i w razie czego przygotowywania materiałów. W samym programie wieloletnim na rzecz osób starszych jest priorytet nr 3 obejmujący zapewnienie bezpiecznego funkcjonowania przy wykorzystywaniu współczesnych narzędzi cyfrowych. Ale patrząc na programy – bo starałam się dotrzeć do niektórych – nie jestem do końca przekonana, czy jest to właściwy kierunek. Zresztą znam głosy, że jeżeli zajęcia dla seniorów prowadzą mężczyźni, lubią się chwalić swoją wiedzą, jeżeli prowadzą kobiety, to z kolei mówią do seniorów jak do czterolatków. A pani profesor bardzo słusznie zwróciła uwagę na to, że prowadzenie zajęć dla seniorów wymaga przede wszystkim profesjonalnej metodyki nauczania, przystosowanej do ich percepcji. Samo sformułowanie „proszę znaleźć ikonę" lub „otworzyć plik" nie jest wystarczającym poleceniem. Należy wytłumaczyć tej grupie osób całą komputerową filozofię. Człowiek starszy patrząc na ekran komputera nie widzi ikon czy plików, tylko ciąg znaków. Trzeba nauczyć go dostrzegania poszczególnych elementów. I tu obawiam się, że osoby młode prowadzące szkolenia powinny same przejść przeszkolenie, jak prowadzić kursy dla seniorów.

Kolejny bardzo ważny cel nr 1 dotyczy także oświaty. Od 2 lat już apeluję o to, żeby się przyjrzeć wreszcie, jak wygląda weryfikacja tych rozlicznych programów, programików, aplikacji i innych technologii informacyjnych i telekomunikacyjnych, czyli tak zwanych tików, które się pojawiły z dnia na dzień w oświacie. One rozdają i rozsiewają dane naszych dzieci na prawo i lewo. Był mój artykuł na ten temat jeszcze w 2020 r. i absolutnie nie dzieje się w tej sprawie nic. Teraz doszły gry. Próbowałam nawet obejrzeć jedną z nich i powstrzymałam się od jej instalacji, bo już mnie zaniepokoiło, gdzie moje dane trafią. Czy gry, które są proponowane w tej chwili przez Ministerstwo Edukacji i Nauki, będą weryfikowane tak jak urządzenia, które mają być stosowane w cyberbezpieczeństwie? Mają być i są badane chociażby przez Instytut Łączności… Czy także oprogramowanie, które de facto będzie obowiązkowe w szkołach, też będzie weryfikowane, gdzie dane trafiają?

Przewodniczący poseł Grzegorz Napieralski (KO):

Pani Joanno, dajmy może szansę panu ministrowi…

Członek Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Jeszcze mam dosłownie dwa slajdy. Są to kolejne bardzo ważne pytania. Jeden pominę. Ale chcę zwrócić uwagę na uczelnie. Są tylko dwie uczelnie z Polski wymienione na stronie ENISA. Nie wiem dlaczego, bo wiem, że więcej uczestniczy w różnego stopnia kształceniu cyberbezpieczników. Na stronie ENISA są podane tylko 2 uczelnie. To też by wymagało weryfikacji.

I na koniec – ostatni slajd u mnie – kwestia kobiet. Ukazała się książka pod patronatem Women4Cyber Foundation – fundacji utrzymywanej ze środków unijnych. Tylko 4 kobiety były i są w niej. W tym ja. Dlatego wiem, że w ogóle coś takiego jest. Tylko 4 Polki. Czy w ogóle są przewidziane jakieś projekty, programy włączenia kobiet do cyberbezpieczeństwa, dania im szansy zaistnienia. Tym bardziej, że raport ENISA z 2021 r. bazujący na tych dwóch uczelniach stwierdza, że zdecydowanie brakuje kobiet w cyberbezpieczeństwie. A wszystkie badania wykazują, że mieszane zespoły cyberbezpieczeństwa pracują dużo lepiej.

W razie czego jedną kwestię poruszę bezpośrednio z panem ministrem. Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, pani Joanno. Panie ministrze, jeszcze nasz doradca się zgłosił. Pana też dopuszczę oczywiście. Zrobimy taką kolejność – doradca, odpowiedź, potem oddaję panu głos. Bardzo proszę.

Stały doradca Komisji Radosław Nielek:

Dzień dobry państwu, dzień dobry panie ministrze. Szanowna Komisjo, to jest bardzo niewdzięczna rola referować postępy w realizacji Strategii Cyberbezpieczeństwa. Bo w zasadzie to jest taki obszar, w którym jeśli nic nie słychać, to znaczy, że jest dobrze. Kiedy pojawiają się problemy, to jest bardzo głośno. Oczywiście incydenty zawsze się będą zdarzać. Nie ma takiej organizacji, takiego systemu, który byłby w stanie sobie poradzić z kompletnym wyeliminowaniem incydentów. Ale oczywiście zawsze warto przyglądać się temu, jak na te incydenty organizacja reaguje. Chciałem się odnieść trochę do tego rozwiązania, mającego zatrzymać i przyciągnąć kadry do szeroko pojętej administracji państwowej w zakresie cyberbezpieczeństwa, o czym pan minister mówił. Oczywiście tam jest katalog instytucji, których to dotyczy. Nie jest też taki obszerny, więc jest pewnie wiele administracji, zwłaszcza na niższym szczeblu, które takiego mechanizmu nie mają, mogą starać się korzystać z jakichś innych, które nie są tak efektywne. Tutaj dwie uwagi –odnosząc trochę się do głosu mojej poprzedniczki.

Dobrze rozumiem w tym rozporządzeniu fakt, że kompetencje dotyczące i certyfikaty dotyczące audytu są wyceniane niżej niż kompetencje i certyfikaty dotyczące praktycznych umiejętności zabezpieczenia systemu teleinformatycznego. Nie wynika to z wartościowania tych kompetencji pod względem tego, ile pracy wymagało ich przyswojenie, tylko bardziej wynika to z wartościowania, jakie rynek nakłada na to. Po prostu ci eksperci, którzy bezpośrednio zajmują się zabezpieczeniem tych systemów teleinformatycznych są w tej chwili natychmiast przez rynek przyciągani na dużo wyższych stawkach niż eksperci, którzy zajmują się audytem na poziomie meta. To niestety jest powszechne dla wielu stanowisk w administracji i także menedżerskich w firmach. Bo doszliśmy do takiego punktu, w którym menedżerowie zarządzający zespołami inżynierów, programistów czasami są wynagradzani gorzej niż członkowie tych zespołów. Nie dlatego, że są mniej wartościowi. Po prostu rynek te kompetencje menedżerskie wycenia niżej niż kompetencje poszczególnych deweloperów. Można oczywiście się z tym nie zgadzać. Można polemizować z rynkiem, ale mechanizm jest po to, żeby przeciwdziałać temu, co rynek powoduje, a nie żeby z nim polemizować. To znaczy, żeby zatrzymać tych ludzi – ja to rozumiem. To mnie tak nie uderza.

Jest pewna rzecz w tym rozporządzeniu. Przy uchwalaniu ustawy właściwie nie było projektu rozporządzenia. Był bardzo takich szczątkowy. Rzuciło mi się w oczy, że tam, zwłaszcza dla tych niższych stanowisk, te wymagane kompetencje i wymagane certyfikaty, przynajmniej niektóre z nich, są, powiedziałbym szczerze, bardzo podstawowe. To znaczy to są certyfikaty możliwe do zdania niewielkim nakładem sił i środków i w zasadzie powinny być zdane przez trochę lepszych studentów albo absolwentów uczelni technicz-

nych i informatycznych. Rozumiem, jak z każdą taką listą, to jest pewna praca, rzeczywistość to weryfikuje. Trzeba pewnie przyjrzeć się, jak to działa. Ale ja mam wrażenie, że trochę konstruując tę listę… Te certyfikaty, stosunkowo proste, wyceniane są przez rynek dość wysoko, więc rozumiem, że w rozporządzeniu się znalazły. Ale przez to rozporządzenie to, rozwiązanie stało się nie takim ekskluzywnym mechanizmem nagradzania zupełnie wybitnych specjalistów, których chcielibyśmy zatrzymać, tylko trochę, mam wrażenie, że zaczyna przypominać to taki mechanizm wynagradzania w ogóle wszystkich, którzy się zajmują cyberbezpieczeństwem, bo po prostu stawki w tej dziedzinie nie przystają do stawek rynkowych. Apeluję nie o zmianę, a raczej o zastanowienie się, czy to powinien być ten mechanizm, czy może ten mechanizm powinien wyglądać inaczej i to powinna być po prostu zwyczajnie siatka płac, być może ze specjalnym rozwiązaniem dla naprawdę wybitnych ekspertów. To tyle, dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję. Panie ministrze, oddaję głos. Później przechodzę do pana. Bardzo proszę.

Sekretarz stanu w KPRM Janusz Cieszyński:

Dziękuję bardzo. Pani poruszyła tak wiele tematów tak szczegółowych, że mam 2 propozycje do wyboru przez panią – tej bardziej racjonalnej. Pierwsza jest taka – po prostu byśmy zaprosili panią na spotkanie i sobie przez te slajdy przeszli – bo jak rozumiem pani miała jakąś prezentację – i po kolei omówili. Mam wrażenie, że poza faktem, że wszystkie te kwestie dotyczą cyberbezpieczeństwa bez wątpienia, trochę chyba odbiegają od takiego meritum naszej dzisiejszej dyskusji. Dlatego myślę, że ewentualnie takie spotkanie pozwoliłoby pewne rzeczy tam wyklarować, odpowiedzieć szczegółowo, a niekoniecznie może na tym forum, na którym jesteśmy dzisiaj.

Jeżeli chodzi o te wypowiedzi dotyczące samej ustawy i wartościowania rozporządzenia – rozumiem, że są jakieś uwagi do tego. Staraliśmy się te różne uwagi zebrać z szerokiego spektrum w trakcie konsultacji. Przyznam, że nie spłynęło ich bardzo dużo. Natomiast tak jak tutaj powiedział pan doradca – od samego początku staraliśmy się kierować tym, jakie są stawki rynkowe, a nie tym, żeby właśnie wartościować względem siebie różne stanowiska. Tutaj chciałem powiedzieć, że to nie jest tak, że to jest rozwiązanie, które jest dla jakiegoś bardzo wąskiego grona ekspertów, jakichś osób super wybitnych, których potrzeba kilka czy kilkanaście, tylko to jest właśnie dokładnie to, o czym pan powiedział, czyli taka pewnego rodzaju siatka płac w cyberbezpieczeństwie. Dlaczego ona jest w ten sposób wdrożona? Przede wszystkim dlatego że to jest ustawa, która ma horyzontalne oddziaływanie na szeroki katalog instytucji, które z tego świadczenia teleinformatycznego korzystają. Propozycja żeby z poziomu takiego aktu prawnego wchodzić w siatki płac wielu instytucji w mojej ocenie byłaby skazana na niepowodzenie. Wiemy doskonale, że to są takie bardzo wrażliwe, kluczowe sprawy dla każdego kierownika jednostki. Są różne reżimy, w których to funkcjonuje. Mamy żołnierzy, mamy funkcjonariuszy, mamy cywili. Bardzo dużo różnych specyficznych uwarunkowań. Dlatego taka formuła. Oczywiście zdaję sobie sprawę z tego, że można powiedzieć, że w niektórych aspektach ona jest niedoskonała. Natomiast patrząc na efekty, uważam, że lepiej zrobić tak i później poprawić – dlatego też jesteśmy w trakcie nowelizowania tej ustawy po tych pierwszych miesiącach funkcjonowania. Właśnie dlatego, żeby uwzględnić te uwagi, które do nas w międzyczasie spłynęły. Uważam, że to jakby był pragmatyczny wybór i powiedziałbym, że korzyści dalece przewyższają ewentualne minusy tego rozwiązania. Tak to oceniam na ten moment.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo dziękuję, panie ministrze, oddaję panu głos, bardzo proszę. Pani Joanno…

Członek Stowarzyszenia ISACA Warszawa Joanna Karczewska:

Chciałam tylko potwierdzić, że bardzo chętnie. To, o czym mówiłam ściśle, przywiązałam do każdego z celów strategii, żeby właśnie nie wychodzić poza ramy dzisiejszego spotkania.

Przewodniczący poseł Grzegorz Napieralski (KO):

Dziękuję bardzo. Proszę bardzo, oddaję panu głos.

Taką pineskę przyłożyć do lewego… I powinno działać.

Koordynator do spraw społeczeństwa informacyjnego i smart city Unii Metropolii Polskich Sylwester Szczepaniak:

2 lata mnie nie było w Sejmie, technologia się zmieniła i już sobie nie radzę. To jest przykład dostosowania cyfrowego.

Dzień dobry. Sylwester Szczepaniak, Unia Metropolii Polskich, koordynatorów spraw społeczeństwa informacyjnego. Mam 4 punkty. Postaram się szybko. Jedna rzecz, do której chciałbym się odnieść, jeżeli chodzi o ustawę wzmacniającą wynagrodzenia w sektorze publicznym – niestety samorządów nie ma w tej ustawie i jeżeli są jakieś prace w przyszłości nad jej nowelizacją, to można się zastanowić, jak ująć jednostki samorządu terytorialnego w tej ustawie. Po to, żeby wystarczyło środków i zabezpieczyć najważniejsze potrzeby w samorządach. Oczywiście znowu tutaj będę mówił głównie o naszych dużych miastach. Dlatego że my działamy w takiej bardziej niekomfortowej dla nas sytuacji. Duże miasto – mówię nie tylko o mieście będącym członkiem Unii Metropolii Polskich, ale nawet 50 tys. obywateli w górę – to jest szereg instytucji i następuje nieuchronna centralizacja na poziomie lokalnym, struktury miasta, informatyki i też cyberbezpieczeństwa. Przemawiają za tym koszty. Centralizacja powoduje większą konieczność ochrony tej infrastruktury, ale też poszukiwania pracowników. Jeszcze do tego jest problem, że w większości tych miast konkurujemy z sektorem prywatnym. A na skutek tej ustawy konkurujemy z sektorem rządowym. Już widać, że pracownicy administracji samorządowej odpowiedzialni za kwestie cyberbezpieczeństwa przechodzą do administracji rządowej, która jest objęta tą ustawą. Mamy więc podwójną rywalizację. Ten fakt jest o tyle niepokojący, że teraz mamy przedłużający się standard związany ze stanami zagrożenia CRB. Widać, że pracowników po prostu brakuje na tych odcinkach, żeby spełnić te wymagania, które są w tych standardach CRB określone. To jest jedna rzecz.

Druga rzecz dotyczy stricte strategii. Proszę państwa, w strategii, która jest obecnie obowiązująca, jednostki samorządu terytorialnego, występują tylko dwa razy. Raz jako przedmiot troski ministra właściwego do spraw informatyzacji w celu szkolenia. Trzeba przyznać, że Ministerstwo Cyfryzacji i NASK w tym zakresie dużo robią. Z informacji, które posiadam, to są setki osób, które zostały przeszkolone z cyberhigieny głównie. Ten kierunek jest jak najbardziej potrzebny i należy go rozwijać. Ale problem pojawia się, jeżeli chodzi o współpracę jednostek samorządu terytorialnego z administracją rządową. I to nawet nie problem komunikacyjny, bo tutaj jakby zrozumienie potrzeb istnieje, tylko instytucjonalny. Na tę chwilę mamy do dyspozycji głównie CSIRT NASK, który jest instrukcją reaktywną. Potrzebujemy większej współpracy instytucjonalnej. To, co my postulujemy, oczywiście jest w KPO i w funduszu europejskich środków. Są przewidziane środki na regionalne SOK-i i tak dalej, ale znowu jeżeli chodzi o samorząd miejski, specyfika jest naprawdę duża. Bo średnio miasto ma 200 jednostek oświatowych plus jednostki organizacyjne pomocy społecznej, plus jednostki inne, które są tworzone na podstawie ustaw. Potrzeby nasze bezpośredniego kontaktu z tym CSIRT-em, z ISACĄ, jeżeli powstanie, lub z tym innym kontraktem, to jest zupełnie inna skala. To nie jest skala małego miasta, małej miejscowości, dla których jak najbardziej… Żeby pokazać skalę na liczbach – zamówienie na program zabezpieczający antywirusowy w mieście, to od 2 mln zł. do 3 mln zł. O takich kwotach mówimy. Oczywiście miasta przygotowują się też do stworzenia po własnej stronie kompetencyjnej coraz większych organizacji. Mowa tutaj o SOK-ach, o kupowaniu usług.

Kolejna rzecz. Mam wrażenie, że strategia, która była przygotowana, nie zauważała pewnej zmiany, która się dzieje na rynku. Dzisiaj była mowa o tym, że będziemy dokonywać dużo dużych inwestycji. Inwestycja w ludzi jak najbardziej. Inwestycja w technologie też. Ale to, z czym my się spotykamy, to zmiana modelu. My już nie możemy kupić pewnych rzeczy, dlatego że nie są oferowane w modelu dostawy, tylko w modelu usługi. I to nas bardzo mocno ogranicza, bo jesteśmy skazani na kilkunastu kluczowych dostawców. Tych, na których nas stać, sami nie chcemy, dlatego, bo nie dają odpowiedniej

gwarancji. Na tych, których byśmy chcieli, nas nie stać. A środki, które są przewidziane w różnych strategiach, są jednak na inwestycje, nie na kupowanie usług.

Ostatnia trzecia rzecz, proszę państwa. Coś, co powstało na samorządowym okrągłym stole we Wrocławiu. Tam był stolik cyberbezpieczeństwa, byli przedstawiciele Departamentu Cyberbezpieczeństwa. Za to dziękujemy. Dyskusja była gorąca, nie we wszystkim się zgodziliśmy. Ale tam pojawiło się coś, co nas uderzyło. Zapominamy o trzecim sektorze. To nawet nie chodzi o każdą jednostkę trzeciego sektora, tylko o jednostki, które za nas, za administrację, zgodnie z ustawą o pożytku publicznym, realizują zadania publiczne. Sektor oświaty w małych i średnich jednostkach samorządu terytorialnego całkowicie jest – nie chcę powiedzieć, że sprywatyzowany – uspołeczniony. Może to będzie lepsze słowo. W ochronie zdrowia za chwilę też się zacznie to dziać. Oni coraz bardziej wspomagają nas w realizacji, a z punktu widzenia strategii i z punktu widzenia ustawy o krajowym systemie cyberbezpieczeństwa są niewidoczni. Jeżeli byśmy mieli w przyszłości o tym myśleć, potrzebujemy wypracować jakiś mechanizm dla tej grupy. To jest postulat nie tylko środowiska NGO-sowego, ale też samorządowego, bo my z tych usług korzystamy. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):

Bardzo panu serdecznie dziękuję. Zróbmy taką samą zasadę – pan minister i wrócę do pana. Dziękuję. Panie ministrze, oddaję panu głos.

Sekretarz stanu w KPRM Janusz Cieszyński:

Dziękuję bardzo. Oczywiście rozumiem, że te potrzeby się pojawiają. Choćby patrząc po samym budżecie – takie duże miasto pewnie jakiś mniejszy dział administracji rządowej przekracza swoją skalą. Pełna zgoda, że tam jest taka potrzeba. Natomiast też szczególnie te duże miasta mają przez ostatnie lata szansę na korzystanie z większych niż kiedykolwiek wcześniej spływów z różnego rodzaju danin publicznych, w szczególności z udziałów swoich w PIT i CIT. Myślę, że to jest doskonały sposób na to, żeby finansować z tego swoje wydatki w tym zakresie. Oczywiście są programy, które uzupełniają – Cyfrowa Gmina czy Cybergmina, którą planujemy w ramach środków z KPO… Natomiast, szanowni państwo, szczególnie mówię o tych wielkich miastach. Jesteśmy w Warszawie , jeżeli kilka milionów złotych kosztuje program antywirusowy, to inwestycje drogowe, które mijamy jadąc do Sejmu z miejsca pracy, są na pewno dużo większej wartości niż środki, które są niezbędne do tego, żeby zapewnić bezpieczeństwo w cyberprzestrzeni instytucjom, które samorząd posiada. Naprawdę zacząłbym podchodzić do tego nie jak do jakiejś ekstrawagancji, czy czegoś dodatkowego. Wydatki na cyberbezpieczeństwo to są takie same wydatki jak na prąd gaz i ochronę. Ciekawe pytanie – ile właśnie taka wielka metropolia wydaje na usługi z zakresu bezpieczeństwa typu ochrona fizyczna obiektów, którymi dysponuje? Czy na to ktoś oczekuje jakichś dodatkowych środków z programów? Nie. Szczególnie, że – tak jak tutaj pan Sylwester słusznie mówi – to przechodzi coraz bardziej w ten model usługowy. Taka jest też rola środków europejskich, że one są zgodne z tą zasadą subsydiarności. Rzeczy ekstra dofinansowujemy ze środków europejskich, a *business as usual* już płacimy z własnego, bieżącego budżetu. Rozumiem, że to są drogie rzeczy, że jest wiele innych wydatków i ja absolutnie tego nie neguję. Sam pracowałem w samorządzie i wiem, że każda złotówka się liczy i jest wiele bardzo potrzebnych rzeczy. Natomiast tutaj raczej nie przewidujemy istotnych zmian w tym zakresie. Podobnie, jeżeli chodzi o kwestie wynagrodzeń. Proszę zauważyć, że jednak ten sektor samorządowy… To byłoby aż, powiedziałbym, dziwne, gdyby zachować tę formułę, którą dzisiaj mamy – rządowe Kolegium do spraw Cyberbezpieczeństwa, na czele którego stoi premier, decydowałoby o tym, ile środków przyznać na wynagrodzenia w urzędach samorządowych… Przyznacie państwo, że to rodziłoby też inne ryzyka. Jeżeli miałbym coś rekomendować, to myślę, że można usiąść do rozmów z… Nie wiem, czy to wydaje MSWiA, czy to jest rozporządzenie premiera w zakresie wynagrodzeń pracowników samorządowych… Żeby utworzyć odpowiednie modyfikacje w widełkach, żeby państwo mogli rzeczywiście zgodnie z tymi regulacjami korzystać z podobnego mechanizmu. Natomiast żeby na to była specjalna pula środków, to nie bardzo sobie wyobrażam taką możliwość. Dziękuję bardzo.

Przewodniczący poseł Grzegorz Napieralski (KO):
Bardzo dziękuję. Oddaję panu głos, bardzo proszę.

Wiceprezes Polskiej Izby Radiodyfuzji Cyfrowej Jacek Kosiorek:
Dziękuję. Jacek Kosiorek. Mam tylko w sumie jedno pytanie, które mnie nurtuje od lat. Czy planowane jest w tej chwili zwiększenie ochrony informacji, jakie zbierają telefony komórkowe? Chodzi o to, że w tej chwili brniemy w taki kierunek, że każdy z nas posiada jeden, może więcej telefonów przy sobie i te dane, które są przekładane na język maszynowy – czyli to, co mówimy nawet w tej chwili przy teoretycznie wyłączonym telefonie – i są rejestrowane w systemach operatora. Również lokalizacja w pionie i w poziomie, na co pozwala 5G i nowsze technologie. Czy planowane jest zwiększenie ochrony tego typu danych, które są dość mocno wykorzystywane przez różne podmioty, niekoniecznie w dobrym kierunku? Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):
Bardzo dziękuję. Panie ministrze?

Sekretarz stanu w KPRM Janusz Cieszyński:
Nie ma takiego przekonania, że można takie dane zgodnie z prawem bez zgody przetwarzać. Zapisy tego, co się dzieje w Sejmie, w publicznym miejscu, może tak. Ale jak rozumiem, tutaj chodzi o zupełnie inne dane, także takie, które są pobierane w trakcie tego, jak przebywamy w domu, czy w pracy, czy w miejscu, gdzie powinniśmy mieć możliwość zachowania prywatności. Jak rozumiem, jest w ten sposób, że część dostawców oprogramowania i sprzętu po prostu ma taką politykę korzystania z tego, która na to pozwala. To na pewno jest zagrożenie niebagatelne. Absolutnie bym nie powiedział, że to nie jest istotne i w tę stronę bym nie szedł. Natomiast wydaje mi się, że trudno jest, szczególnie na poziomie krajowym, wprowadzić jakieś istotne ograniczenia, które byłyby egzekwowalne. Widzimy na przykładzie DSA, że jeżeli jest konsensus na poziomie Unii Europejskiej, to jesteśmy w stanie pewne gwarancje użytkownikom Internetu zapewnić. Uważam, że to jest krok w dobrą stronę. Czy gdybyśmy my, jako Polska, próbowali przeprowadzić regulacje tego rodzaju, które obowiązywałyby wyłącznie w Polsce, osiągnęlibyśmy sukces? No, śmiem wątpić. Myślę, że po prostu dostawcy tego sprzętu powiedzieliby nam – nie będziemy po prostu w Polsce sprzedawać. Absolutnie nie bagatelizuję tego. Natomiast myślę, że niwą do załatwiania tych spraw jest arena międzynarodowa. Jak mówiłem, my tego nie... Nie tak dawno… Można zobaczyć, że strukturach departamentu cyberbezpieczeństwa kancelarii premiera intensywnie rozbudowujemy ten pion odpowiedzialny za relacje międzynarodowe. Zależy nam na tym, żeby być tam, gdzie jest rozwój tych technologii i żeby aktywnie działać na rzecz tego, żeby dbać o prywatność, dbać o prawa indywidualnych użytkowników, dbać o prawo małych i średnich przedsiębiorców, o których mówił pan poseł Kapinos. To są rzeczywiście takie podmioty, które w starciu z tym wielkim biznesem technologicznym bez skutecznego wsparcia instytucji publicznych są bez szans. Trzeba mieć tego pełną świadomość.

Wiceprezes PIRC Jacek Kosiorek:
Dziękuję. Tylko jeszcze jedno takie doprecyzowanie. Pamiętam wypowiedź jednego z dużych operatorów telekomunikacyjnych w Polsce, który śmiał się z mównicy, czy z pulpitu konferencyjnego i powiedział, że nawet wie, kiedy klient buty wiąże w mieszkaniu. Przy pochyleniu telefonu kompas w nim zamontowany pozwala na wiele informacji, które są dla nas istotnie. Wiadomo, że to jest temat trudny i bardzo szeroki. Pojawienie się z telefonem komórkowym w danym miejscu też jest analizowane. Ale prośba gorąca o przeanalizowanie tego tematu. Bo to jest według mnie bardzo istotne. Komputer możemy włączyć, wyłączyć i on te dane albo sprzeda, albo nie, albo ktoś ściągnie te dane, albo nie. Natomiast telefon komórkowy działa 24 godziny na dobę. Chyba nikt z nas przy tym stole nie wyłącza telefonu nawet na noc. Wydaje się, że to jest temat bardzo trudny i szeroki. Nie chcę za długo zabierać głosu. Dziękuję serdecznie.

Przewodniczący poseł Grzegorz Napieralski (KO):
Dziękuję bardzo. Pani minister?

Sekretarz stanu w KPRM Janusz Cieszyński:

Dziękuję.

Przewodniczący poseł Grzegorz Napieralski (KO):

Czy ktoś z państwa jeszcze chciałby zabrać głos, zadać pytanie? Nie słyszę. Zamykam dyskusję. Bardzo dziękuję panie ministrze za wypowiedź, za odpowiedzi, za przybycie. Panu prezesowi Oko również bardzo dziękuję za przybycie i obecność na dzisiejszym posiedzeniu.

Na tym wyczerpaliśmy porządek dzienny. Zamykam posiedzenie Komisji. Do zobaczenia.